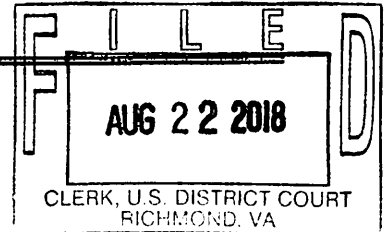


AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH account
"scottshot2308@gmail.com," STORED AT PREMISES
CONTROLLED BY DROPBOX, INC

Case No. 3:18SW202

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Information associated with "scottshot2308@gmail.com," which is more particularly described in Attachment A of the attached Affidavit and hereby incorporated by reference as if fully stated herein.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B of the attached Affidavit, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 2252A

Receipt and Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit, incorporated herein by reference.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Lynette K. Stull, FBI TFO

Printed name and title

Sworn to before me and signed in my presence.

Date:

8/22/2018

City and state:

Richmond, VA

Is/

Roderick C. Young
United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:
INFORMATION ASSOCIATED WITH
DROPBOX ACCOUNT
scottshot2308@gmail.com,
THAT IS STORED AT PREMISES
CONTROLLED BY DROPBOX, INC.

Case No. 3:18SW202

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Lynette K. Stull, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for content and records associated with Dropbox user account scottshot2308@gmail.com which is stored at premises owned, maintained, controlled or operated by Dropbox Incorporated at 333 Brannan Street, San Francisco, California, 94107. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox Incorporated to disclose to the government copies of the information (including the content of communication) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. Your affiant been a sworn police officer with Chesterfield County Police for over

ten years and have been a detective for almost five of those years. I am assigned to Criminal Investigation, Special Victims Unit. I am also currently assigned as a Task Force Officer (TFO) to the Federal Bureau of Investigation, Richmond Division Child Exploitation Task Force and have been since 2015. I have participated in investigations involving sexual assault, preferential child molesters, persons who produce, collect, and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training in the areas of sexual assaults and child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers.

3. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code, Sections 2251, 2252 and 2252A involving child exploitation offenses.

4. I have been deputized as a Special Deputy United States Marshal since July 2015. As a Special Deputy United States Marshal, your Affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A, receipt and distribution of child pornography, is present in the information associated with above-listed Dropbox account

– scottshot2308@gmail.com. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

7. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

RELEVANT CRIMINAL STATUTES

8. **Receipt and Distribution of Child Pornography:** 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

9. **Child pornography** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexual explicit conduct. *See* 18 U.S.C. § 2256(8).

10. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

11. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

12. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

TECHNICAL INFORMATION REGARDING DROPBOX

13. Dropbox is a file hosting service that offers cloud-based storage of electronic files, file synchronization, personal cloud, and client software. Dropbox makes it possible for a user to have access to saved files without the requirement of storing those files on a particular desktop computer or other electronic storage device. Once installed, Dropbox creates a special folder on the user's computer, the contents of which are then synchronized to Dropbox's servers and to other computers and devices on which the user has installed Dropbox, keeping the same files up-to-date on all devices. Dropbox is available to install and use on a variety of platforms and operating systems, including Microsoft Windows, Apple OS, Linux, as well as smartphones and tablets running the Apple iOS, Android and Windows Phone operating systems. Because of this cloud-based storage model, a user can store files in his or her Dropbox account(s) and those files would not be physically present on the user's home computer or smartphone. Put another way, anyone searching the computer of an individual who has stored files in a Dropbox account

would not be able to view these files if the user opted only to store them at an offsite such as Dropbox.

14. Pertinent to this investigation, in my training and experience I have learned that individuals often store evidence of crimes, including contraband child pornography images, in cloud-based file storage systems like Dropbox for the purpose of adding additional layers of security and anonymity.

15. Dropbox provides a variety of online services, including online storage access, to the general public. Users may obtain a basic account that provides 2 gigabytes of storage space at no charge. For a fee, users can obtain Dropbox accounts with significantly greater storage capacity. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

16. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer or mobile device, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

17. Online storage providers like Dropbox typically retain certain transactional

information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

18. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

PROBABLE CAUSE

19. On February 14, 2018, Special Agent/Child Exploitation Task Force Officer John P. Houlberg, began an investigation into distributors of child pornography over the Internet. On February 14, 2018, between 16:08 PM and 16:15 PM EST, SA Houlberg successfully downloaded child pornography from the dynamic IP address "73.147.221.97," over a P2P network on the Internet using an automated software program used to search P2P networks. This software program is a free version of the P2P program "BitTorrent" that has been configured to record packet traffic, display geographic locations of IP addresses, and download files from a single source (single source refers to downloading from a single IP address, as opposed to

multiple IP addresses as the default P2P configuration for most P2P applications).

20. The BitTorrent network is a very popular and publicly available P2P file sharing network. Most computers that are part of this network are referred to as “peers” or “clients”. A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publically available and are typically free P2P client software programs that can be downloaded from the Internet.

21. Law enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

22. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator’s BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client’s IP address, 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program, and 3) the BitTorrent network

client program and version being utilized by the suspect computer. The law enforcement client program has the ability to log this information.

23. Your affiant reviewed the evidence and observed that the automated program successfully achieved a direct connection with IP address 73.147.221.97, on February 14, 2018, between 16:08 PM and 16:15 PM EST. The automated program browsed the BitTorrent files being shared by that IP address during the undercover session on February 14, 2018, at 16:08 PM EST through 16:15 PM EST. Such browsing was conducted using SHA1 hash values.¹ Based on known child pornography SHA1 values, the automated program successfully downloaded 812 BitTorrent files.

24. Your affiant reviewed the downloaded file information and capture logs, which revealed that the download on February 14, 2018, between 16:08 PM EST and 16:15 PM EST, occurred solely from the dynamic IP address 73.147.221.97. Your affiant conducted a check of the American Registry for Internet Numbers ("ARIN") and determined that Comcast Cable Communications, LLC. holds the registration for IP address 73.147.221.97.

25. I reviewed the aforementioned files to determine whether they contained child pornography. Based on my training, experience and review of those images, I determined that there were multiple image files that constituted child pornography, specifically, the lascivious exhibition of the genitals, as those terms are defined under federal law. Two of the files are described below:

- a. **lsm04-01-039.jpg** is a color image, depicting two prepubescent females,

¹ Previously identified child pornography photographs that are widely circulated on the Internet will, if unaltered, always have the same hash values, which enables investigators to quickly identify other instances of the same offending images.

approximately 8 to 10 years-old. The children are nude and lying on the sand by the water. The first child is lying on her back on what appears to be a leopard print style blanket. She has her knees slightly bent and spread open, exposing her vagina to the camera. She has what appears to be an apple in her right hand. The second child is kneeling, facing towards the other child. Her legs are spread a part and her vagina is exposed for the camera. She has a partially eaten banana in her right hand and the fingers of her left hand are inserted in the mouth of the other child.

- b. **lsm04-03-061.jpg** is a color image of what appears to be part of the same series of the image described earlier. This image depicts two prepubescent females, approximately 8 to 10 years-old. The children are nude and appear to be outdoors. The children are on their hands and knees on top of a blanket. They are side by side and have their heads upside down, facing the camera. Their legs are spread open, exposing their vaginas for the camera. Their vaginas are the focal point of the picture.

26. Based on this information, an administrative subpoena was submitted to Comcast Cable Communication, LLC. on February 15, 2018, requesting subscriber information for the Comcast user-assigned IP address 73.147.221.97, for the aforementioned timeline, during which the files of child pornography were shared.

20. Results from the administrative subpoena revealed the following information about IP address 73.147.221.97 during the aforementioned time frame: (1) the subscriber was "Terry Perry", (2) the address listed for the account was 13110 Deepark Drive, Midlothian, Virginia, 23112 (hereinafter, "SUBJECT PREMISES"), and (3) the listed email address was

TERRY-PERRY@comcast.net. Comcast records indicated that the dynamic IP address 73.147.221.97 was assigned to the SUBJECT PREMISES beginning on August 25, 2017, through February 16, 2018. Additionally, on July 2, 2018, a second administrative subpoena requesting subscriber information for IP address 73.147.221.97 was submitted to Comcast Cable Communication, LLC. Results received indicated that the IP address 73.147.221.97 was still currently assigned to SUBJECT PREMISES as of June 29, 2018.

RESULTS OF JULY 25, 2018, SEARCH WARRANT

21. On July 24, 2018, United States Magistrate Judge David J. Novak issued a search warrant, Case No. 3:18SW181, for the residence of Terry Perry located at 13110 Deepark Drive, Midlothian, Virginia, 23112. On July 25, 2018, agents from the FBI and task force officers executed the Federal search warrant at approximately 6:00 AM.

22. Upon execution of the search warrant, Scott Kesler, a resident of the premises, was interviewed by your Affiant and FBI TFO John Houlberg. Scott Kesler admitted that he had a Dropbox folder on his laptop that contained child pornography. Scott Kesler signed a Consent to Assume Online Identity authorization form and advised that he used scottshot2308@gmail.com to access the Dropbox account.

23. An on-scene preview of digital items seized from the room of Scott Kesler pursuant to the federal search warrant revealed child pornography on his red HP laptop computer that was contained in the Dropbox account associated with scottshot2308@gmail.com. The following video found in the Dropbox account is described below:

vicki-bondage.avi

The video depicts a female approximately 10 years-old, fully nude except for white lace thigh-high stockings. The female's wrists are bound with black rope. She has

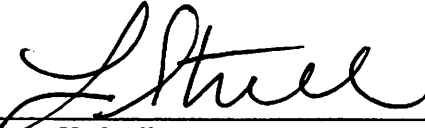
similar rope tied around her neck which appears to be connected to rope tied around her ankles from the back. She is wearing a black mask covering the top half of her face. Approximately 1:23 into the video, an adult male, wearing a white t-shirt but nude from the waist down unties her hands slightly, grabs the rope and forces what appears to be a flesh colored plastic penis into her mouth. The male then forces his penis into her mouth. At approximately 5 minutes the video pans and shows the same juvenile female laying on her back with her legs spread and bound to the side with the black rope and her arms tied up above her head. The adult male penetrates her vagina then again puts his penis in her mouth.

CONCLUSION

24. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of Dropbox there exists evidence of violations 18 U.S.C. § 2252A, within the above-listed Dropbox accounts. Accordingly, a search warrant is requested.

25. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” *See* 18 U.S.C. § 2711(3)(A)(i).

26. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.



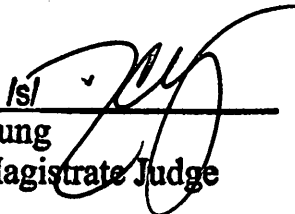
Lynette K. Stull
Special Deputy United States Marshal
FBI Child Exploitation Task Force
Chesterfield County Police Department

SEEN



Samuel E. Fishel
Special Assistant United States Attorney

SUBSCRIBED and SWORN
before me on August 22, 2018.



/s/ Roderick C. Young
United States Magistrate Judge